# STORAGE DEVICE FOR BACKING UP CRYPTOGRAPHIC KEY

**Publication number:** JP2001103045 (A)
**Publication date:** 2001-04-13
**Inventor(s):** TSURUMARU JUNICHIRO +
**Applicant(s):** ADVANCED MOBILE TELECOMM SECUR +
**Classification:**
**- international:** ***G06F12/14; G06F12/16; G06F21/06; G06F21/24; H04L9/08; H04L9/10;*** **G06F12/14; G06F12/16; G06F21/00; H04L9/08; H04L9/10;** (IPC1-7): G06F12/14; H04L9/08; H04L9/10
**- European:**
**Application number:** JP19990276798 19990929
**Priority number(s):** JP19990276798 19990929

Abstract of **JP 2001103045 (A)**

PROBLEM TO BE SOLVED: To prevent backup file of cryptographic keys from being physically decoded easily and also to recover cryptographic keys, even if a part of the cryptographic keys fails. SOLUTION: A plurality of communication cryptographic keys used for communication are stored in a tamper-proof key memory 13. Secret information A and B are respectively stored in tamper-proof information A memory and information B memory 15, which are different from the memory 13. A cipher- calculating part 12 generates a cryptographic key for backup from the information A and B, enciphers a plurality of communication cryptographic keys and stores them in a backup file 18. In the case of recovery, the enciphered communication cryptographic keys are decoded with the cryptographic key for backup. Safety can be enhanced, because the communication cryptographic keys cannot be decoded unless obtaining the plurality of memory information and the backup file.